National Infrastructure Advisory Council (NIAC)

The Insider Threat to Critical Infrastructures

Thomas Noonan
General Manager
IBM Internet Security Systems

Edmund Archuleta
General Manager
El Paso Water Utilities

Overview

- Objective
- Scope
- NIAC Participation
- Study Group
  - Critical Sectors Represented
- Progress
- Approach/ Work Breakdown

Objective

- To define the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization.
- The second phase of the study will focus on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts.
- Completion of the study will produce recommendations for improving operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders.

Scope

- Scope of the study (as outlined in the January 16 letter from Secretary Chertoff):
  - ✓ Define the "insider threat" physical and cyber, including potential consequences, economic or otherwise
  - ✓ Analyze the dynamics and scope of the insider threat including critical infrastructure vulnerabilities
  - ✓ Analyze the potential impact of globalization on the critical infrastructure marketplace and insider issues
  - ✓ Identify/define the obstacles to addressing the insider threat
  - ✦ Identify issues, potential problems, and consequences associated with screening employees
  - ✦ Identify legal, policy, and procedural barriers aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators
  - ✦ Identify and make policy recommendations on potential remedies for addressing the insider threat (up to and including potential legislation)

NIAC Participation

- Co-chairs:
  - Mr. Thomas Noonan, IBM Internet Security Systems
  - Mr. Edmund Archuleta, El Paso Water Utilities
- Other NIAC members include:
  - Mr. John Thompson, Symantec
  - Ms. Margaret Grayson, Grayson and Associates

The Group is seeking further NIAC member participation in the study.

Study Group

Currently includes:

- 12 security professionals from major infrastructure operators
- Balance of IT and physical security focus, diverse viewpoints
- 10 Critical Infrastructure Sectors Represented

Critical Sectors Represented

- Critical sectors include:
  - Chemical
  - Commercial Facilities*
  - Dams
  - Energy (Oil and Gas sub-sector)
  - Energy (Electricity sub-sector)
  - Financial Services
  - Food and Agriculture
  - Information Technology
  - Nuclear
  - Transportation
  - Water

*Invited

Progress

- Early Working Group meetings validated approach, work breakdown and Study Group focus on
  - Two-phased approach
  - Phase 1 will seek to define the Insider Threat and develop recommendations for addressing it
  - Phase 2 will address the legal, policy, and procedural issues that arise in mitigating insider threats, including personal privacy legal issues associated with employee screening

- Study Group work to date
  - Study Group meeting - Study Group orientation
  - Concept development meeting - initial definition of terms and tasks
  - Operational Concept meeting - task breakdown and near-term work assignments

Approach and Work Breakdown

January	Initial research; draft restatement of the problem (complete)
February	Vet the restated problem and gain additional background materials; begin study group recruitment (complete)
March	Continue recruitment; organize group and assign tasks (complete)
	BEGIN PHASE I
April	Develop refined milestones for *Phase I* (underway)
May to July	*Phase I* research, including input from Study Group stakeholders; develop outline for final product; provide status report to NIAC at July meeting (upcoming)
Aug. to Oct.	Complete *Phase I* research; outline all secondary phase issues and their impact; draft recommendations; publish coordinating draft of report; provide NIAC Quarterly status report on progress and Working Group draft recommendations to NIAC
	BEGIN PHASE II
Sep. to Jan.	Begin research and compile findings for report**
Nov. to Dec.	Finalize *Phase I* report January 2008 - Deliver report with cover letter

Questions?